Information Sciences 677 (2024) 120878

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

INFORMATION SCIENCES

Secure consensus for multiagent systems with hybrid cyber attacks: A multi-round-robin protocol-based approach [☆]

Jinliang Liu [a], Hao Zheng [b], Lijuan Zha [c,*], Engang Tian [d], Chen Peng [e]

[a] *School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, Jiangsu, 210044, China*
[b] *College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, Jiangsu, 210023, China*
[c] *College of Science, Nanjing Forestry University, Nanjing, Jiangsu, 210037, China*
[d] *School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, 200093, China*
[e] *School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, 200444, China*

ARTICLE INFO

Keywords:
Multiagent systems (MASs)
Multi-Round Robin Protocol (MRRP)
Scheduling protocol
Cyber attack

ABSTRACT

This article addresses secure consensus of discrete multiagent systems (DMASs) with information exchange under Multi-Round Robin Protocol (MRRP). Since the information exchange among agents is via the constrained networked transmission channel, it implies that the communication resources should be fully utilized. To overcome this issue, MRRP is employed to adjust the data packet transmissions and conserve the limited network resources. Considering that the transmitted signals may be tampered by malicious attacks during transmission process, an new control strategy is presented taking the negative effects of the deception and injection attacks into account. Based on the augmented system model, a sufficient condition is attained. Moreover, the distributed controller gain is obtained such that the DMASs reach consensus with definite bound in mean-square sense. One simulation example is exploited to demonstrate the validity of the acquired consensus control strategy.

1. Introduction

In recent years, multiagent systems (MASs) have aroused much interest of many researchers in various research fields including multivehicle systems [1–3], satellite cluster [4], intelligent grid [5–9], complex network [10,11], and coupled oscillators [12]. The goal of consensus control problem of MASs is to design a distributed controller to make the controlled agents keep relatively stable and reach consistent state. Researchers of different disciplines have participated in the research extensively, and a considerable number of valuable results have been achieved so far (see e.g., [13–16]).

Note that the execution of data transmission and control protocols is via shared networks in MASs, which has advantages of flexibility and extensibility. However, due to the fragility of the communication networks, the information exchange among agents is easily tampered or interrupted by cyber attacks, which may damage the performance of the controlled system. How to ensure the security of MASs is a crucial issue that is of paramount importance. Nowadays, researchers pay more and more attention on network

[☆] This work was supported by the National Natural Science Foundation of China under Grant 62373252 and Grant 62273174, Natural Science Foundation of Jiangsu Province of China under Grant BK20230063, and Startup Foundation for Introducing Talent of NUIST under Grant 2024r063.

[*] Corresponding author.
E-mail address: zhalijuan@vip.163.com (L. Zha).

https://doi.org/10.1016/j.ins.2024.120878
Received 16 March 2024; Received in revised form 17 April 2024; Accepted 3 June 2024

Available online 7 June 2024

attacks and have made some preliminary achievements, such as [17–24]. The authors in [18] investigated the event-triggered impulsive control for complex networks under deception attacks. In [23], to cope with denial-of-service attacks, an adaptive fault-tolerant controller was derived for event-trigger heterogeneous MASs with actuator faults. Noted that these results referred above only involve one type of cyber attack, which does not consider that the attacker may employ different attack means to compromise the MASs. It is still challenging to develop consensus control method for MASs which can tolerant the multiple, random and mixed network attacks.

On the other hand, the communication among different agents over networks is constrained by the limited the network bandwidth. If all the agents gain access to the network at each time, data collisions are inevitable encountered [25], which may lead to channel fading [26], communication delay [27–30] and even degrade system performance. Hence, it is necessary to implement effective ways to coordinate the information transmission of the agents and avoid the negative effects induced by the constrained network bandwidth [31–35]. Fortunately, some communication protocols have been applied to schedule the signal transmission in the recently published results [36]. For example, in [37], the authors researched the distributed $\mathcal{H}_\infty$ consensus of a type of MASs with Stochastic Communication Protocol. In [38], [39], [40] and [41], Weighted Try-Once-Discard (WTOD) protocol was implemented to achieve reasonable dispatch of the information transmission. Based on Round Robin (RR) Protocol, in [13], the $\mathcal{H}_\infty$ bipartite consensus algorithm on finite-horizon was discussed for cooperation-competition MASs. In [42], the recursive filtering problem for multisensor multirate networked systems with cyber attacks is discussed, where the RRP and fading measurements are considered. However, the communication protocols above enable only one channel transmission. When the number of agent clusters increases, the communication efficiency will decrease conspicuously, so the communication frequency needs to be multiplied for maintaining the stability of the system. Therefore, for regulating the sequence of the transmitted data on the network, an enhanced communication protocol is required.

In this paper, with consideration of the optimized utilization of the limited network resources and the hybrid cyber-attacks, the secure consensus control of MASs will be dealt with based on information exchange subject to MRRP. The following is a summary of the main highlights of this article:

1. Different from the results which avoid network conflicts and congestion by using WTOD protocol [39] and RR protocol [13], the adopted MRRP in this paper enables multiple neighbor agents of agent i to have access to the network simultaneously instead of just one agent accessible for the network, which is more flexible in making arrangements for network transmissions and conserving limited network resources.
2. The negative effects of the hybrid cyber-attacks on the MASs are investigated, which is more general than some existing results [23,43,44], where one type of cyber-attacks is considered. It is assumed that the transmitted sensor measurements and the controller output are transmitted via unreliable communication networks, which are subject to randomly injection attacks.
3. A sufficient condition is derived which can ensure the expected consensus of the addressed MASs with MRRP and hybrid cyber-attacks. Simulation results show the designed consensus controller can ensure the discussed MASs under MRRP is immune to the hybrid cyber-attacks.

The rest of this article is organized as follows. The modeling of the discussed DMASs is introduced in section 2. In Section 3, a sufficient condition is derived to achieve the desired consensus of the DMASs and the controllers gains are obtained. A simulation example is given in Section 4, illustrating the effectiveness of the results. Finally, Section 5 is the conclusion of this paper.

Notations: Some notations in this paper are given below, others are common standard. I and I_N represent identity matrix with compatible dimensions and identity matrix with N dimensions, respectively. $\circ$ is the Hadamard product, of which the product is defined as $[A \circ B]_{ij} = A_{ij} B_{ij}$.

2. Problem formulation

Due to the high dependence of the information exchange in MASs, the limited communication and the vulnerability of the network should be taken into account. Since the energy consumption is huge in MASs, in this paper, the network resource occupancy and the negative effects of the cyber attacks will be considered. This article aims to develop a control strategy to guarantee the consensus of the MASs with MRRP and hybrid cyber attacks.

2.1. Graph topology

Throughout this article, $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{H})$ denotes the communication topology of the considered MASs with order N. $\mathcal{V} = \{1, 2, \cdots, N\}$ and $\mathcal{E} = \mathcal{V} \times \mathcal{V}$ represent the set of agents and the set of edges, respectively. And $\mathcal{H} = [h_{ij}]$ is an adjacency matrix with non-negative elements, in which $h_{ij} > 0 \iff (i,j) \in \mathcal{E}$, while $h_{ij} = 0 \iff (i,j) \notin \mathcal{E}$. (i,j) denotes an undirected edge of $\mathcal{G}$, which means that the information from the agent j can be received by agent i. Self-edges (i,i) are not allowed in this paper, i.e., $(i,i) \notin \mathcal{E}$ and $h_{ii} = 0$ for any $i \in \mathcal{V}$. $\mathcal{L} \triangleq \mathcal{H} - \mathcal{D} = [l_{ij}]$ is defined as the Laplacian matrices of the undirected graph $\mathcal{G}$, where $\mathcal{D} = diag\{d_1, d_2, \cdots, d_N\}$ is the degree matrix with $d_i = \sum_{j \in \mathcal{N}_i} h_{ij}$. For each agent $i \in \mathcal{V}$, $\mathcal{N}_i \triangleq \{j \in \mathcal{V} : (i,j) \in \mathcal{E}\}$ represents the neighbor agents of agent i.

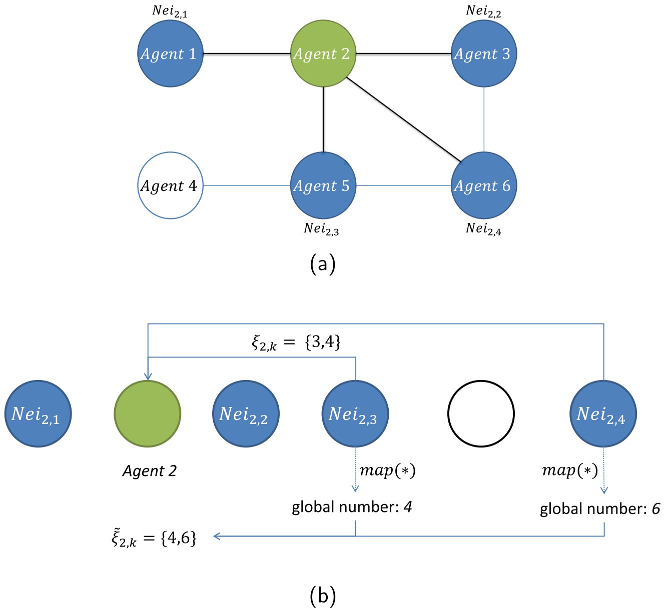


Fig. 1. $map(*)$ function demonstration. (1a) Communication graph and neighbor set (1b) Mapping demonstration.

2.2. Problem formulation

Consider the following DMASs with N homogeneous agents, the dynamics of agent i is:

$$\begin{cases} x_{i,k+1} = Ax_{i,k} + Bu^*_{i,k} \\ y^j_{i,k} = C(x_{j,k} - x_{i,k}), \quad j \in \mathcal{N}_i \end{cases} \tag{1}$$

where A, B and C are known matrices, $x_{i,k} \in \mathbb{R}^n$ and $u^*_{i,k} \in \mathbb{R}^p$ represent the state and real control input of agent i, respectively. $y^j_{i,k} \in \mathbb{R}^q$ is the relative measurement outputs from its neighbor j.

To schedule network resource reasonably for avoidance of data collision and the waste of bandwidth, we introduce MRRP in this article which is utilized to govern the order of the agent nodes granted for data transmission. Denote $\xi_{i,k}$ as the set of the active nodes, the value of which determines which sensor nodes obtain permission for data transmission. In the MRRP, $\xi_{i,k}$ can be designed as:

$$\xi_{i,k} = \{mod((k-1)*S_i, N_i)+1, mod((k-1)*S_i, N_i)+2, \cdots, mod((k-1)*S_i, N_i)+S_i\} \tag{2}$$

where the function $mod(x, Y)$ represents the non-negative remainder of x divided by the integer Y, S_i represents the quantity of selected neighbors which transmit data to agent i. The elements in $\xi_{i,k}$ are represented as $nei_{i,1}, nei_{i,2}, \cdots, nei_{i,S_i}$. Furthermore, by defining $map(*)$ as map function, which map the *-th selected neighbor of agent i to its global number in all agents, we could map selected neighbor number set to all nodes number set, then

$$\widetilde{\xi}_{i,k} = \left\{ map(nei_{i,1}), map(nei_{i,2}), \cdots, map(nei_{i,S_i}) \right\} \tag{3}$$

Remark 1. The correspondence between the set of neighbor node numbers and the set of global node numbers is explained as follows. As shown in Fig. 1, there exist 6 agents labeled as $\{1, 2, \cdots, 6\}$. In Fig. 1(a), taking agent 2 as an example, it has 4 neighbors represented by blue solid circles and noted as $Nei_{2,1}, Nei_{2,2}, Nei_{2,3}, Nei_{2,4}$. In Fig. 1(b), agent 2 communicates with $Nei_{2,3}$ and $Nei_{2,4}$ at instant k, that is, $\xi_{2,k} = \{3,4\}$. By the use of $map(*)$, the set of selected neighbor $\xi_{2,k} = \{3,4\}$ is mapped to the set $\widetilde{\xi}_{2,k} = \{4,6\}$.

Noting the periodic character of MRRP, we have

$$\xi_{i,k} = \xi_{i,k+t_i} \quad \widetilde{\xi}_{i,k} = \widetilde{\xi}_{i,k+t_i}$$

where

$$t_i = \frac{[N_i, S_i]}{S_i} \tag{4}$$

in which $[a, b]$ represents least common multiple.

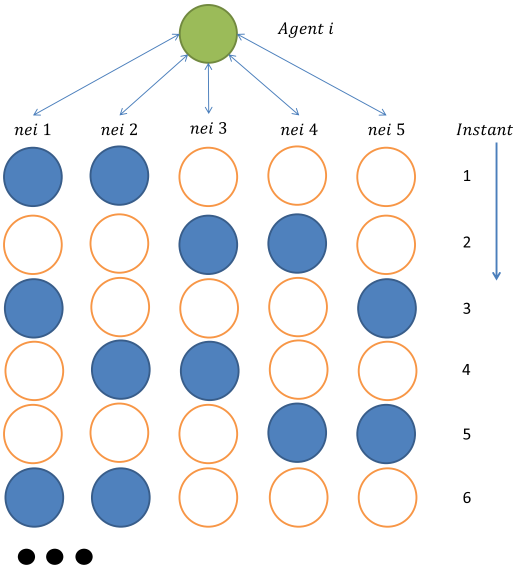


Fig. 2. MRRP demonstration.

Remark 2. In order to understand MRRP more clearly, one example is given to explain the periodicity of information transmission. As shown in Fig. 2, agent i has 5 neighbor agents ($nei_1, \cdots, nei_5$) and communicate with 2 neighbor agents at one instant. That is, $N_i = 5$, $S_i = 2$. The selected neighbor agents which obtain permission to release packets to agent i are represented by blue solid circles, while the hollow circle represents that there is no information transmission. As time changes, the set of selected neighbor numbers cycles in the order of $\{nei_1, nei_2\}$, $\{nei_3, nei_4\}$, $\{nei_5, nei_1\}$, $\{nei_2, nei_3\}$, $\{nei_4, nei_5\}$, which indicates $t_i = 5$, as shown in formula (4).

According to the node connectivity under MRRP, the update matrix is depicted by:

$$\Phi_{\xi_{i,k}} = row\{\sum_{i\in\tilde{\xi}_{i,k}} \delta(i-1), \sum_{i\in\tilde{\xi}_{i,k}} \delta(i-2), \cdots, \sum_{i\in\tilde{\xi}_{i,k}} \delta(i-N)\}, \tag{5}$$

in which $\delta(\cdot) \in \{0,1\}$ is the Kronecker delta function.

Under MRRP, the update strategy is

$$y_{i,k} = \sum_{j\in\tilde{\xi}_{i,k}} l_{ij} y^j_{i,k} \tag{6}$$

Notice that the measurement output can be tampered by deception attacks stochastically before arriving observer i. Under possible deception attacks, the real observer input $y^*_{i,k}$ is

$$y^*_{i,k} = (1-\lambda_{i,k})y_{i,k} + \lambda_{i,k}\overline{h}_{i,k} \tag{7}$$

where $\overline{h}_{i,k}$ is the attack signal, $\lambda_{i,k}$ are adopted to characterize occurrence of the attacks. Considering the limitation of resources and the concealment of attacks, there is a new hypothesis:

$$\|\overline{h}_{i,k}\|_2 \le \|My_{i,k}\|_2 = h_i, \tag{8}$$

where M and h_i are known matrix with appropriate dimensions. $\lambda_{i,k} = 0$ represents there are no deception attacks. $\lambda_{i,k} = 1$ means the deception attacks are in presence. $\lambda_{i,k}$ takes the values in {0,1}, and follows the following probability distribution: $Pr\{\lambda_{i,k} = 0\} = 1 - \overline{\lambda}_i$, $Pr\{\lambda_{i,k} = 1\} = \overline{\lambda}_i$, $0 \le \overline{\lambda}_i \le 1$ for any i.

Introduce T as the least common multiple of $t_1, t_2, \cdots, t_N$. Denote $\tau_{i,k} = \sum_{j\in\tilde{\xi}_{i,k}} l_{ij}(x_{j,k} - x_{i,k})$. Then the observer and controller are devised as

$$\begin{cases} \hat{\tau}_{i,k+1} = \hat{A}_{r(k)}\hat{\tau}_{i,k} + \hat{L}_{r(k)}y^*_{i,k} \\ u_{i,k} = \hat{K}_{r(k)}\hat{\tau}_{i,k} \end{cases} \tag{9}$$

where $r(k) = mod(k-1, T) + 1$, and $\hat{A}_{r(k)}$, $\hat{L}_{r(k)}$, $\hat{K}_{r(k)}$ are gain matrices being designed.

Assume that the distributed controller output $u_{i,k}$ may be modified by injection attack stochastically before arriving agent i. Considering the possible injection attacks, the real received controller input $u^*_{i,k}$ are modeled by

$$u^{*}_{i,k}=u_{i,k}+\theta_{i,k}u^{a}_{i,k} \tag{10}$$

where $u^{a}_{i,k}$ is attack function of $u_{i,k}$ at time k, which is decided by the attacker, $\theta_{i,k}$ is a random variable which is used to describe the occurrence of the attacks. Considering the limitation of resources and the concealment of attacks, it is assumed that:

$$\|u^{a}_{i,k}\|_2\leq\|Ou_{i,k}\|_2=u_i \tag{11}$$

where O and u_i are known matrix with appropriate dimensions. $\theta_{i,k}=0$ represents there are no deception attacks. $\theta_{i,k}=1$ means the deception attacks are in presence. $\theta_{i,k}$ takes the values in the set {0,1}, and obeys following probability distribution: $Pr\{\theta_{i,k}=0\}=1-\overline{\theta}_i$, $Pr\{\theta_{i,k}=1\}=\overline{\theta}_i$, $0\leq\overline{\theta}_i\leq 1$ for any i.

Remark 3. From attacker's perspective, the attacks need energy, so the attack intensity is upper bounded, which is reflected in the bounded Euclidean norm of the deception data or the injection data. Secondly, the frequency of attacks should not be too high. Too frequent attacks are easy to expose the existence of attacks, thus reducing the concealment of deception or injection attacks, and it is difficult to effectively achieve the target system to operate in the direction expected by the attacker. From the perspective of defender, the attack is random. The defender cannot predict the attack time of the attacker, but on the whole, the attacks satisfy a certain probability distribution during the operation of the system. Given the above analysis, it is reasonable to assume (8) and (11).

For the convenience of the following further derivation, denote

$$\Lambda_k=diag\left\{\lambda_{1,k},\cdots,\lambda_{N,k}\right\},\quad \Theta_k=diag\left\{\theta_{1,k},\theta_{2,k},\cdots,\theta_{N,k}\right\},\quad x_k=col\left\{x_{i,k}\right\},\quad \hat{\tau}_k=col\left\{\hat{\tau}_{i,k}\right\}$$

$$\Phi_{\xi_k}=\begin{bmatrix}\Phi_{\xi_{1,k}}\\ \cdots\\ \Phi_{\xi_{N,k}}\end{bmatrix},\quad \widetilde{\Phi}_{\xi_k}=diag\{\sum_{j\in\widetilde{\xi}_{i,k}}l_{ij}\},\quad L^{\Phi}_{r(k)}=L\circ\Phi_{\xi_k}-\widetilde{\Phi}_{\xi_k},\quad u^{a}_{k}=col\left\{u^{a}_{i,k}\right\},\quad \overline{H}_k=col\left\{\overline{h}_{i,k}\right\}$$

Remark 4. In DMASs with a relatively fixed topology, the Laplacian matrix of them is also relatively fixed. By introducing Laplacian matrix, the analysis difficulty of DMASs will be greatly reduced. However, in this paper, due to the introduction of MRRP, the communication among the nodes of DMASs presents periodic changes, that is, the topology structure of the DMASs changes periodically, and is no longer fixed, so the usual Laplacian matrix no longer work here. To deal with that, we construct Φ_{ξ_k} and $\widetilde{\Phi}_{\xi_k}$ to generate $L^{\Phi}_{r(k)}$ here, which also has the properties of Laplace matrix in the following analysis.

Substitute (6), (7) into (9) and substitute (10) into (1), respectively, we obtain:

$$x_{i,k+1}=Ax_{i,k}+B\hat{K}_{r(k)}\hat{\tau}_{i,k}+\theta_{i,k}Bu^{a}_{i,k} \tag{12}$$

$$\begin{aligned}\hat{\tau}_{i,k+1}&=\hat{A}_{r(k)}\hat{\tau}_{i,k}+\lambda_{i,k}\hat{L}_{r(k)}\overline{h}_{i,k}+[(I-\Lambda_k)(L\circ\Phi_{\xi_k})]_i\otimes\hat{L}_{r(k)}Cx_k-[(I-\Lambda_k)(\widetilde{\Phi}_{\xi_k})]_i\otimes\hat{L}_{r(k)}Cx_k\\&=\hat{A}_{r(k)}\hat{\tau}_{i,k}+\lambda_{i,k}\hat{L}_{r(k)}\overline{h}_{i,k}+[(I-\Lambda_k)L^{\Phi}_{r(k)}]_i\otimes\hat{L}_{r(k)}Cx_k\end{aligned} \tag{13}$$

where $[\bullet]_i$ represents a row vector the elements of which are the ith row of matrix $\bullet$. According to the definition of x_k and $\hat{\tau}_k$, we get

$$\begin{cases}x_{k+1}&=I\otimes Ax_k+I\otimes B\hat{K}_{r(k)}\hat{\tau}_k+\Theta_k\otimes Bu^{a}_k\\ \hat{\tau}_{k+1}&=I\otimes\hat{A}_{r(k)}\hat{\tau}_k+\Lambda_k\otimes\hat{L}_{r(k)}\overline{H}_k+[(I-\Lambda_k)L^{\Phi}_{r(k)}]\otimes\hat{L}_{r(k)}Cx_k\end{cases} \tag{14}$$

Definition 1. [43] DMASs (1) is said to reach consensus with bound U in mean-square sense (MSS), if there exist positive scalar U, the initial value satisfies $\sum_{i=1}^{N}\parallel x_{i,0}-\frac{1}{N}\sum_{j=1}^{N}x_{j,0}\parallel_2^{\,2}\leq\chi_0^2$, such that

$$\mathbb{E}\{\parallel x_{i,k}-x_{j,k}\parallel_2{}^2\}\leq U,\ \forall i,j\in\mathcal{V},k\geq 0. \tag{15}$$

3. Main results

In the following, by resorting to some appropriate model transformations, the dynamics of the closed-loop system will be firstly derived. Based on this model, the sufficient condition is provided guaranteeing the consensus of the MASs. Then, a control algorithm is designed to achieve the expected consensus performance.

3.1. Preliminaries

With the intention of designing consensus controller, some proper treatment is necessary by making some targeted transformation of (1). The average state of all agents and the deviation between each state and the average state are respectively defined as:

$$\overline{x}_k=\frac{1}{N}\sum_{i=1}^{N}x_{i,k}=\frac{1}{N}(\mathbf{1}^{\top}\otimes I)x_k$$

$$\widetilde{x}_{i,k} = x_{i,k} - \overline{x}_k$$

in which each element of "**1**" is one and "**1**" stands for a compatible dimension vector. It can be obtained easily that

$$\overline{x}_{k+1} = A\overline{x}_k + \frac{1}{N}(\mathbf{1}^\top \otimes B\hat{K}_{r(k)})\hat{\tau}_k + \frac{1}{N}(\mathbf{1}^\top\Theta_k \otimes B)u_k^a \tag{16}$$

$$\widetilde{x}_{k+1} = x_{k+1} - (\mathbf{1} \otimes I)\overline{x}_{k+1} = (I \otimes A)\widetilde{x}_k + [\mathbb{N} \otimes (B\hat{K}_{r(k)})]\hat{\tau}_k + (\mathbb{N}\Theta_k \otimes B)u_k^a \tag{17}$$

where $\mathbb{N} = [n_{ij}]_{N\times N}$ with

$$n_{ij} = \begin{cases} 1 - \frac{1}{N} & i = j \\ -\frac{1}{N} & i \neq j \end{cases}$$

Similarly, define

$$\overline{\tau}_k = \frac{1}{N}\sum_{i=1}^{N}\hat{\tau}_{i,k} = \frac{1}{N}(\mathbf{1}^\top \otimes I)\hat{\tau}_k$$

$$\widetilde{\tau}_{i,k} = \hat{\tau}_{i,k} - \overline{\tau}_k$$

Similar to the derivation of (16) and (17), it can be obtained that

$$\begin{aligned}\overline{\tau}_{k+1} &= \frac{1}{N}\{I \otimes \hat{A}_{r(k)}\hat{\tau}_k + \Lambda_k \otimes \hat{L}_{r(k)}\overline{H}_k + [(I-\Lambda_k)L^{\Phi}_{r(k)}] \otimes \hat{L}_{r(k)}Cx_k\} \\ &= \hat{A}_{r(k)}\overline{\tau}_k + \frac{1}{N}(\mathbf{1}^\top\Lambda_k \otimes \hat{L}_{r(k)}\overline{H}_k) + \frac{1}{N}[\mathbf{1}^\top(I-\Lambda_k)L^{\Phi}_{r(k)}] \otimes \hat{L}_{r(k)}Cx_k\end{aligned} \tag{18}$$

$$\begin{aligned}\widetilde{\tau}_{k+1} &= \{I \otimes \hat{A}_{r(k)}\hat{\tau}_k + \Lambda_k \otimes \hat{L}_{r(k)}\overline{H}_k + [(I-\Lambda_k)L^{\Phi}_{r(k)}] \otimes \hat{L}_{r(k)}Cx_k\} \\ &\quad - (\mathbf{1} \otimes I)\hat{A}_{r(k)}\overline{\tau}_k + \frac{1}{N}(\mathbf{1}^\top\Lambda_k) \otimes \hat{L}_{r(k)}\overline{H}_k) + \frac{1}{N}[\mathbf{1}^\top(I-\Lambda_k)L^{\Phi}_{r(k)}] \otimes \hat{L}_{r(k)}Cx_k]\} \\ &= (I \otimes \hat{A}_{r(k)})\widetilde{\tau}_k + (\mathbb{N}\Lambda_k \otimes \hat{L}_{r(k)})\overline{H}_k + [\mathbb{N}(I-\Lambda_k)L^{\Phi}_{r(k)}] \otimes \hat{L}_{r(k)}Cx_k\end{aligned} \tag{19}$$

Notice the relation $\mathbb{N} \otimes (B\hat{K}_{r(k)})\hat{\tau}_k = \mathbb{N} \otimes (B\hat{K}_{r(k)})\widetilde{\tau}_k = I \otimes (B\hat{K}_{r(k)})\widetilde{\tau}_k$ and $\mathbf{1}^\top(I-\Lambda_k)L^{\Phi}_{r(k)}\mathbf{1} = 0$. Then, with the aid of (17) and (19), the DMASs (14) can be further rewritten as

$$\begin{cases} \widetilde{x}_{k+1} = (I \otimes A)\widetilde{x}_k + I \otimes (B\hat{K}_{r(k)})\widetilde{\tau}_k + (\mathbb{N}\Theta_k \otimes B)u_k^a \\ \widetilde{\tau}_{k+1} = (I \otimes \hat{A}_{r(k)})\widetilde{\tau}_k + (\mathbb{N}\Lambda_k \otimes \hat{L}_{r(k)})\overline{H}_k + [\mathbb{N}(I-\Lambda_k)L^{\Phi}_{r(k)}] \otimes \hat{L}_{r(k)}C\widetilde{x}_k \end{cases} \tag{20}$$

Furthermore, by introducing the variables

$$\widetilde{\Theta}_k = \Theta_k - \overline{\theta}I \tag{21}$$

$$\widetilde{\Lambda}_k = \Lambda_k - \overline{\lambda}I \tag{22}$$

Then substitute (21) and (22) into (20), one has

$$\begin{cases} \widetilde{x}_{k+1} = & (I \otimes A)\widetilde{x}_k + I \otimes (B\hat{K}_{r(k)})\widetilde{\tau}_k + \mathbb{N}\widetilde{\Theta}_k \otimes Bu_k^a + \overline{\theta}\mathbb{N} \otimes Bu_k^a \\ \widetilde{\tau}_{k+1} = & (I \otimes \hat{A}_{r(k)})\widetilde{\tau}_k + (\mathbb{N}\widetilde{\Lambda}_k \otimes \hat{L}_{r(k)})\overline{H}_k + \overline{\lambda}\mathbb{N} \otimes \hat{L}_{r(k)}\overline{H}_k \\ & +(1-\overline{\lambda})\mathbb{N}L^{\Phi}_{r(k)} \otimes \hat{L}_{r(k)}C\widetilde{x}_k - \mathbb{N}\widetilde{\Lambda}_k L^{\Phi}_{r(k)} \otimes \hat{L}_{r(k)}C\widetilde{x}_k \end{cases} \tag{23}$$

Define $\eta_k = [\ \widetilde{x}_k^\top \quad \widetilde{\tau}_k^\top\,]^\top$, the DMASs (23) can eventually be written as

$$\eta_{k+1} = (\mathcal{A}_{1,r_k r} + \mathcal{A}_{2,k})\eta_k + (\mathcal{D}_{1,r(k)} + \mathcal{D}_{2,k})\overline{\varpi}_k \tag{24}$$

where

$$\mathcal{A}_{1,r(k)} = \begin{bmatrix} I \otimes A & I \otimes B\hat{K}_{r(k)} \\ (1-\overline{\lambda})\mathbb{N}L^{\Phi}_{r(k)} \otimes \hat{L}_{r(k)}C & I \otimes \hat{A}_{r(k)} \end{bmatrix}, \quad \mathcal{A}_{2,k} = \begin{bmatrix} 0 & 0 \\ -\mathbb{N}\widetilde{\Lambda}_k L^{\Phi}_{r(k)} \otimes \hat{L}_{r(k)}C & 0 \end{bmatrix},$$

$$\mathcal{D}_{1,r(k)} = \begin{bmatrix} \overline{\theta}\mathbb{N} \otimes B & 0 \\ 0 & \overline{\lambda}\mathbb{N} \otimes \hat{L}_{r(k)} \end{bmatrix}, \quad \mathcal{D}_{2,k} = \begin{bmatrix} \mathbb{N}\widetilde{\Theta}_k \otimes B & 0 \\ 0 & \mathbb{N}\widetilde{\Lambda}_k \otimes \hat{L}_{r(k)} \end{bmatrix}.$$

3.2. *Consensus analysis*

In the following, the consensus analysis of (24) will be performed. Under the support of Lyapunov stability theorem, the sufficient condition ensuring the mean-square consensus of (24) with a certain bound will be presented.

Theorem 1. *Given $\mathcal{G}$, $\widetilde{A}_{r_k}$, $\widetilde{L}_{r_k}$ and $\widetilde{K}_{r_k}$. If there exist s $\mathcal{P}_{r_k} > 0$, positive scalars γ_{r_k}, and positive scalar ϵ, for any $r_k = 1, 2, \cdots, T$, satisfying*

$$(1+\epsilon)\mathcal{A}_{1,r_k}^{\top}\mathcal{P}_{r_{k+1}}\mathcal{A}_{1,r_k} + \overline{\mathcal{A}}_{2,k}^{\top}\mathcal{P}_{r_{k+1}}\overline{\mathcal{A}}_{2,k} - \mathcal{P}_{r_k} + \gamma_{r_k} I < 0 \tag{25}$$

then the studied controlled DMASs (24) is consensus in MSS with bound

$$max\{\frac{2\rho_{max}\mathcal{X}_0^2}{\rho_{min}}, \frac{\mu\Psi}{\mu - 1}\} \tag{26}$$

where

$$\mathcal{P}_{r_k} = \begin{bmatrix} I \otimes P_{r_k}^{(1)} & * \\ I \otimes P_{r_k}^{(0)} & I \otimes P_{r_k}^{(2)} \end{bmatrix}, \quad \overline{\mathcal{A}}_{2,k} = \begin{bmatrix} 0 & 0 \\ \sqrt{\overline{\lambda}(1-\overline{\lambda})}\mathbb{N}L_{r_k}^{\Phi} \otimes \hat{L}_{r_k}C & 0 \end{bmatrix},$$

$$\rho_{max} = max\{\lambda_{max}(\mathcal{P}_{r_k})\}, \quad \rho_{min} = \lambda_{min}(\mathcal{P}_T), \quad \mu = \frac{\rho_{max}}{\rho_{max} - \gamma_{min}}, \quad \gamma_{min} = min\{\gamma_{r_k}\}, \quad r_k = r(k),$$

$$\Psi = max\{\lambda_{max}(\Omega_{r_k})\sum_{i=1}^{N}(u_i + h_i)\}, \quad \Omega_{r_k} = (1+\epsilon^{-1})(\mathcal{D}_{1,r_k}^{\top}P_{r_{k+1}}\mathcal{D}_{1,r_k}) + \mathcal{D}_{2,k}^{\top}P_{r_{k+1}}\mathcal{D}_{2,k}.$$

Proof. Construct Lyapunov function shown below:

$$V_k = \eta_k^{\top}\mathcal{P}_{r_k}\eta_k$$

Along the trajectory of (24), taking the mathematical expectation of the difference of V_k, one has

$$\begin{aligned} \mathbb{E}\{\Delta V_k\} &= \mathbb{E}\{V_{k+1}\} - V_k \\ &= \eta_k^{\top}(\mathcal{A}_{1,r_k}^{\top}\mathcal{P}_{r_{k+1}}\mathcal{A}_{1,r_k} - \mathcal{P}_{r_k} + \mathbb{E}\{\mathcal{A}_{2,k}^{\top}\mathcal{P}_{r_{k+1}}\mathcal{A}_{2,k}\})\eta_k \\ &\quad + \overline{\varpi}_k^{\top}(\mathcal{D}_{1,r_k}^{\top}\mathcal{P}_{r_{k+1}}\mathcal{D}_1 + \mathcal{D}_{2,k}^{\top}\mathcal{P}_{r_{k+1}}\mathcal{D}_{2,k})\overline{\varpi}_k + 2\eta_k^{\top}\mathcal{A}_{1,r_k}^{\top}\mathcal{P}_{r_k}\mathcal{D}_{1,r_k}\overline{\varpi}_k \end{aligned} \tag{27}$$

By calculation, one has

$$\mathbb{E}\{(-\mathbb{N}\widetilde{\Lambda}_k L_{r_k}^{\Phi})^{\top}(-\mathbb{N}\widetilde{\Lambda}_k L_{r_k}^{\Phi})\} = \overline{\lambda}(1-\overline{\lambda})L_{r_k}^{\Phi\,\top}\mathbb{N}L_{r_k}^{\Phi} \tag{28}$$

According to the inequality $2a^{\top}b \leq \epsilon a^{\top}a + \epsilon^{-1}b^{\top}b$, one has

$$2\eta_k^{\top}\mathcal{A}_{1,r_k}^{\top}\mathcal{P}_{r_k}\mathcal{D}_{1,r_k}\overline{\varpi}_k \leq \epsilon\eta_k^{\top}\mathcal{A}_{1,r_k}^{\top}\mathcal{P}_{r_{k+1}}\mathcal{A}_{1,r_k}\eta_k + \epsilon^{-1}\overline{\varpi}_k^{\top}\mathcal{D}_{1,r_k}^{\top}P_{r_{k+1}}\mathcal{D}_{1,r_k}\overline{\varpi}_k$$

Thus, the formula (27) is transformed into

$$\begin{aligned} \mathbb{E}\{\Delta V_k\} &\leq \eta_k^{\top}\{(1+\epsilon)\mathcal{A}_{1,r_k}^{\top}\mathcal{P}_{r_{k+1}}\mathcal{A}_{1,r_k} + \overline{\mathcal{A}}_{2,k}^{\top}\mathcal{P}_{r_{k+1}}\overline{\mathcal{A}}_{2,k} - \mathcal{P}_{r_k} + \gamma_{r_k} I\}\eta_k \\ &\quad + \overline{\varpi}_k^{\top}\{(1+\epsilon^{-1})(\mathcal{D}_{1,r_k}^{\top}P_{r_{k+1}}\mathcal{D}_{1,r_k}) + \mathcal{D}_{2,k}^{\top}P_{r_{k+1}}\mathcal{D}_{2,k}\}\overline{\varpi}_k - \gamma_{r_k}\mathbb{E}\{\|\eta_k\|_2^{\;2}\} \\ &\leq -\gamma_{r_k}\eta_k^{\top}\eta_k + \lambda_{max}(\Omega_{r_k})\sum_{i=1}^{N}(u_i + h_i) \\ &\triangleq -\gamma_{r_k}\eta_k^{\top}\eta_k + \Psi_{r_k} \end{aligned} \tag{29}$$

Due to $\Psi = max\{\Psi_{r_k}\}$, one has

$$\begin{aligned} \mathbb{E}\{\Delta V_k\} &\leq -\gamma_{r_k}\eta_k^{\top}\eta_k + \Psi \\ &\leq -\gamma_{min}\eta_k^{\top}\eta_k + \Psi \end{aligned} \tag{30}$$

Then, for any $\mu > 1$, one can get

$$\begin{aligned} \mu^{k+1}\mathbb{E}\{V_{k+1}\} - \mu^k\mathbb{E}\{V_k\} &\leq \mu^{k+1}\mathbb{E}\{\Delta V_k\} + \mu^k(\mu - 1)\mathbb{E}\{V_k\} \\ &\leq (\rho_{max}(\mu - 1) - \gamma_{min}\mu)\mu^k\mathbb{E}\{\|\widetilde{\eta}_k\|_2^{\;2}\} + \mu^{k+1}\Psi \end{aligned} \tag{31}$$

If there exists a positive scalar μ satisfying $\rho_{max}(\mu - 1) - \gamma_{min}\mu = 0$, we get

$$\begin{aligned} \mu^k\mathbb{E}\{V_k\} - \mathbb{E}\{V_0\} &= \sum_{s=1}^{k}\{\mu^s\mathbb{E}\{V_s\} - \mu^{s-1}\mathbb{E}\{V_{s-1}\}\} \\ &\leq \sum_{s=1}^{k}\mu^s\Psi \end{aligned} \tag{32}$$

which implies

$$\begin{aligned}\mathbb{E}\{V_k\} &\leq \mu^{-k}\mathbb{E}\{V_0\} + \sum_{s=1}^{k}\mu^{s-k}\Psi \\ &= \mu^{-k}\mathbb{E}\{V_0\} + \frac{(1-\mu^{-k})\Psi}{1-\mu^{-1}} \\ &= \mu^{-k}(\mathbb{E}\{V_0\} - \frac{\mu\Psi}{\mu-1}) + \frac{\mu\Psi}{\mu-1} \\ &\leq max\{\mathbb{E}\{V_0\}, \frac{\mu\Psi}{\mu-1}\}\end{aligned} \tag{33}$$

Notice

$$\begin{aligned}\| x_{i,k} - x_{j,k} \|_2{}^2 &\leq \| \widetilde{x}_k \|_2{}^2 \\ &\leq \| \widetilde{x}_k \|_2{}^2 + \| \widetilde{\tau}_k \|_2{}^2 = \| \eta_k \|_2{}^2\end{aligned} \tag{34}$$

with $\| \eta_0 \|^2 \leq \mathcal{X}_0^2$. Combining formula (33) and (34), the controlled DMASs (24) is consensus in MSS with bound

$$max\{\frac{2\rho_{max}\mathcal{X}_0^2}{\rho_{min}}, \frac{\mu\Psi}{\mu-1}\} \quad \square \tag{35}$$

Remark 5. Since η_k and $\overline{\omega}_k$ are coupled to each other, the inequality $2a^\top b \leq \epsilon a^\top a + \epsilon^{-1} b^\top b$ is implemented in the proof for handling coupling items. Note that in Theorem 1, due to periodicity, the number of γ_{r_k} and ϵ should have been T, but through appropriate selection of basic inequality parameters for the convenience of subsequent analysis, a common ϵ can be used to replace $\epsilon_1, \epsilon_2, \cdots, \epsilon_T$. However, γ_{r_k} should not be arbitrarily changed to the expected parameters, otherwise it will increase the conservativeness of sufficient condition proposed. In Theorem 2, similar treatment method was carried out.

3.3. Distributed controller design

Through the discussion in above section, it is proved that the DMASs can reach bounded stability under the condition that inequality (25) is true. In this chapter, the main purpose is to adopt appropriate methods to solve the unknown controller and obtain the controller gain according to Theorem 1.

Theorem 2. *For given $\widetilde{\epsilon}$ ($\widetilde{\epsilon} > 1$) and undirected communication graph $\mathcal{G}$. If there exist $\mathcal{P}_{r_k} > 0$, some matrices Λ_{r_k}, Δ_{r_k}, $\widetilde{A}_{r_k}$, $\widetilde{L}_{r_k}$, $\widetilde{K}^*_{r_k}$ and positive scalars γ_{r_k}, for any $r_k = 1, 2, \cdots, T$, satisfying*

$$\begin{bmatrix} \hat{\mathcal{F}}_{0,r_k} & (*) & (*) \\ \hat{\mathcal{F}}_{1,r_k} & \hat{\mathcal{F}}_{3,r_k} & (*) \\ \hat{\mathcal{F}}_{2,r_k} & 0 & \hat{\mathcal{F}}_{3,r_k} \end{bmatrix} < 0 \tag{36}$$

where

$$\mathcal{P}_{r_k} = \begin{bmatrix} \hat{P}_{1,r_k} & (*) \\ \hat{P}_{0,r_k} & \hat{P}_{2,r_k} \end{bmatrix}, \quad \hat{P}_{1,r_k} = I \otimes P_{1,r_k}, \quad \hat{P}_{2,r_k} = I \otimes P_{2,r_k}, \quad \hat{P}_{0,r_k} = I \otimes P_{0,r_k}, \quad r_k = r(k),$$

$$\hat{\mathcal{F}}_{0,r_k} = \begin{bmatrix} -\hat{P}_{1,r_k} + \hat{\gamma}_{r_k} & (*) \\ -\hat{P}_{0,r_k} & -\hat{P}_{2,r_k} + \hat{\gamma}_{r_k} \end{bmatrix}, \quad \hat{\mathcal{F}}_{1,r_k} = \begin{bmatrix} \widetilde{\epsilon}\hat{\Delta}_{r_k}\hat{X}_A + \widetilde{\epsilon}(1-\overline{\lambda})(\mathbb{N}L^{\Phi}_{r_k} \otimes I_n)\widetilde{L}_{r_k}\hat{C} & \widetilde{\epsilon}(\widetilde{K}^*_{r_k} + \widetilde{A}_{r_k}) \\ \widetilde{\epsilon}(1-\overline{\lambda})(\mathbb{N}L^{\Phi}_{r_k} \otimes I_n)\widetilde{L}_{r_k}\hat{C} & \widetilde{\epsilon}\widetilde{A}_{r_k} \end{bmatrix},$$

$$\Delta_{r_k} = \begin{bmatrix} \Delta_{1,r_k} & \Delta_{2,r_k} \\ 0 & \Delta_{3,r_k} \end{bmatrix}, \quad \hat{\Delta}_{r_k} = I_N \otimes \Delta_{r_k}, \quad X = \begin{bmatrix} B(B^\top B)^{-1} & B^\perp \end{bmatrix}^\top, \quad \hat{X}_A = I_N \otimes XA,$$

$$\hat{\gamma}_{r_k} = I_{(n*N)} \otimes \gamma_{r_k}, \quad \hat{C} = I_N \otimes C, \quad \hat{X} = I_N \otimes X, \quad \hat{\Lambda}_{r_k} = I_N \otimes \Lambda_{r_k},$$

$$\widetilde{K}^*_{r_k} = I_N \otimes \hat{K}^*_{r_k}, \quad \hat{K}^*_{r_k} = \Delta_{r_k} XB\hat{K}_{r_k} \tag{37}$$

$$\widetilde{A}_{r_k} = I_N \otimes (\Lambda_{r_k}\hat{A}_{r_k}) \tag{38}$$

$$\widetilde{L}_{r_k} = I_N \otimes (\Lambda_{r_k}\hat{L}_{r_k}) \tag{39}$$

$$\hat{\mathcal{F}}_{2,r_k} = \begin{bmatrix} \sqrt{\overline{\lambda}(1-\overline{\lambda})}(\mathbb{N}L^{\Phi}_{r_k} \otimes I_n)\widetilde{L}_{r_k}\hat{C} & 0 \\ \sqrt{\overline{\lambda}(1-\overline{\lambda})}(\mathbb{N}L^{\Phi}_{r_k} \otimes I_n)\widetilde{L}_{r_k}\hat{C} & 0 \end{bmatrix}, \quad \hat{\mathcal{F}}_{3,r_k} = \begin{bmatrix} \mathcal{J}_{1,r_k} & (*) \\ \mathcal{J}_{0,r_k} & \mathcal{J}_{2,r_k} \end{bmatrix}$$

$$\mathcal{J}_{1,r_k} = \hat{P}_{1,r_{k+1}} - \hat{\Delta}_{r_k}\hat{X} - [\hat{\Delta}_{r_k}\hat{X}]^\top, \quad \mathcal{J}_{2,r_k} = \hat{P}_{2,r_{k+1}} - \hat{\Lambda}_{r_k} - \hat{\Lambda}^\top_{r_k}, \quad \mathcal{J}_{0,r_k} = \hat{P}_{0,r_{k+1}} - \hat{\Lambda}^\top_{r_k}$$

Then, from (38), (39) and (37), $\hat{A}_{r_k}$, $\hat{L}_{r_k}$, $\hat{K}_{r_k}$ can be derived, respectively, and the controlled DMASs (24) is consensus in MSS with the bound (26).

Proof. By Schur complement lemma, inequality (25) is equivalent to

$$\begin{bmatrix} -\mathcal{P}_{r_k}+\gamma_{r_k}I & (*) & (*) \\ \widetilde{\epsilon}\mathcal{A}_{1,r_k} & -\mathcal{P}_{r_{k+1}}^{-1} & (*) \\ \overline{\mathcal{A}}_{2,k} & 0 & -\mathcal{P}_{r_{k+1}}^{-1} \end{bmatrix} < 0 \tag{40}$$

where $\mathcal{A}_{1,r_k}$, $\overline{\mathcal{A}}_{2,k}$ have been defined in equation (24) and (25) respectively.

Set

$$\hat{\mathcal{W}}_{r_k} = \begin{bmatrix} I\otimes\Delta_{r_k}X & I\otimes\Lambda_{r_k} \\ 0 & I\otimes\Lambda_{r_k} \end{bmatrix} \tag{41}$$

Pre-multiplying (40) with diag $\{I, \hat{\mathcal{W}}_{r_k}, \hat{\mathcal{W}}_{r_k}\}$ and post-multiplying inequality (40) with diag $\{I, \hat{\mathcal{W}}_{r_k}^{\top}, \hat{\mathcal{W}}_{r_k}^{\top}\}$, it is obtained that

$$\begin{bmatrix} -\mathcal{P}_{r_k}+\gamma_{r_k}I & (*) & (*) \\ \widetilde{\epsilon}\hat{\mathcal{W}}_{r_k}\mathcal{A}_{1,r_k} & \widetilde{\mathcal{Q}}_{r_k} & (*) \\ \hat{\mathcal{W}}_{r_k}\overline{\mathcal{A}}_{2,k} & 0 & \widetilde{\mathcal{Q}}_{r_k} \end{bmatrix} < 0 \tag{42}$$

where

$$\widetilde{\mathcal{Q}}_{r_k} = -\hat{\mathcal{W}}_{r_k}\mathcal{P}_{r_{k+1}}^{-1}\hat{\mathcal{W}}_{r_k}^{\top}$$

Denote

$$\mathcal{F}_{3,r_k} = \mathcal{P}_{r_{k+1}} - \hat{\mathcal{W}}_{r_k}^{\top} - \hat{\mathcal{W}}_{r_k}$$

Due to

$$-\hat{\mathcal{W}}_{r_k}\mathcal{P}_{r_{k+1}}^{-1}\hat{\mathcal{W}}_{r_k}^{\top} - \mathcal{P}_{r_{k+1}} + \hat{\mathcal{W}}_{r_k}^{\top} + \hat{\mathcal{W}}_{r_k} = (\hat{\mathcal{W}}_{r_k} - \mathcal{P}_{r_{k+1}})\mathcal{P}_{r_{k+1}}^{-1}(\hat{\mathcal{W}}_{r_k}^{\top} - \mathcal{P}_{r_{k+1}}) \le 0 \tag{43}$$

one can obtain that (42) is satisfied if

$$\begin{bmatrix} \mathcal{F}_{0,r_k} & (*) & (*) \\ \mathcal{F}_{1,r_k} & \mathcal{F}_{3,r_k} & (*) \\ \mathcal{F}_{2,r_k} & 0 & \mathcal{F}_{3,r_k} \end{bmatrix} < 0 \tag{44}$$

where

$$\mathcal{F}_{0,r_k} = -\mathcal{P}_{r_k} + \gamma_{r_k}I$$

$$\mathcal{F}_{1,r_k} = \widetilde{\epsilon}\hat{\mathcal{W}}_{r_k}\mathcal{A}_{1,r_k} \triangleq \begin{bmatrix} \mathcal{Q}_{11,r_k} & \mathcal{Q}_{12,r_k} \\ \mathcal{Q}_{21,r_k} & \mathcal{Q}_{22,r_k} \end{bmatrix}, \quad \mathcal{F}_{2,r_k} = \begin{bmatrix} \sqrt{\overline{\lambda}(1-\overline{\lambda})}\mathbb{N}L_{r_k}^{\Phi}\otimes\Lambda_{r_k}\hat{L}_{r_k}C & 0 \\ \sqrt{\overline{\lambda}(1-\overline{\lambda})}\mathbb{N}L_{r_k}^{\Phi}\otimes\Lambda_{r_k}\hat{L}_{r_k}C & 0 \end{bmatrix}$$

$$\mathcal{Q}_{11,r_k} = \widetilde{\epsilon}I_N\otimes\Delta_{r_k}XA + \widetilde{\epsilon}(1-\overline{\lambda})\mathbb{N}L_{r_k}^{\Phi}\otimes\Lambda_{r_k}\hat{L}_{r_k}C, \quad \mathcal{Q}_{12,r_k} = \widetilde{\epsilon}I_N\otimes\Delta_{r_k}XB\hat{K}_{r_k} + \widetilde{\epsilon}I_N\otimes\Lambda_{r_k}\hat{A}_{r_k}$$

$$\mathcal{Q}_{21,r_k} = \widetilde{\epsilon}(1-\overline{\lambda})\mathbb{N}L_{r_k}^{\Phi}\otimes\Lambda_{r_k}\hat{L}_{r_k}C, \quad \mathcal{Q}_{22,r_k} = \widetilde{\epsilon}I_N\otimes\Lambda_{r_k}\hat{A}_{r_k}$$

By using the property of Kronecker function, (44) is equivalent to (36). The proof is completed. □

Remark 6. So far, the secure consensus problem of MASs under limited network resources and cyber attacks has been dealt with, where the sensor measurement and the control input are subject to cyber-attacks. The employed MRRP can optimize the communications among the agents in MASs with constrained network bandwidth. The influences of the cyber attacks that intend to mislead the system are reflected on the sensor measurement and the control input. To attenuate the threat of the cyber attacks as well as optimize constrained network bandwidth, a new consensus controller is proposed that possess attack tolerant capability of the hybrid attacks and can ensure the expected performance.

4. Simulation example

In the following, we will verify the effectiveness of the proposed consensus control strategy for the DMASs subject to MRRP and hybrid cyber attacks. There are six agents in this simulation example, whose interaction topology is shown in Fig. 3. Assume the communication network with MRRP is prone to cyber attacks.

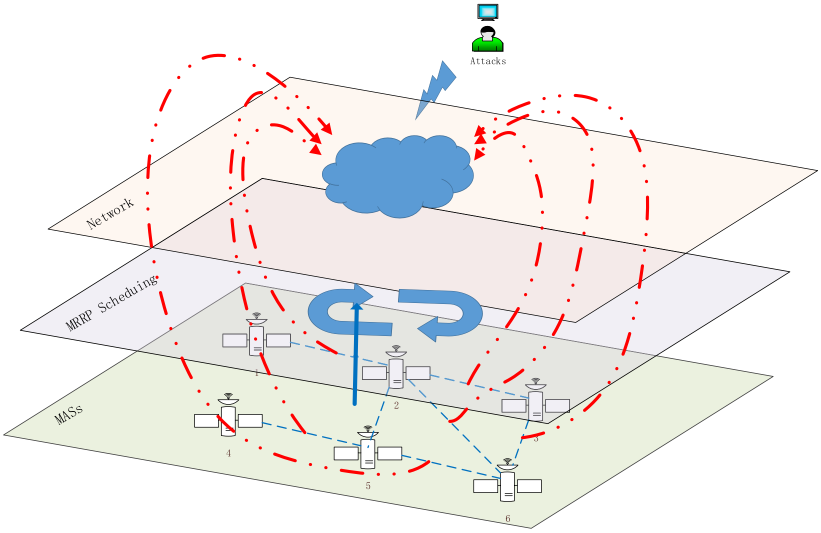


Fig. 3. Framework of the MASs.

Choose the system matrices of (1) as

$$A=\begin{bmatrix}1 & 0.1\\ 0 & 1\end{bmatrix}, B=\begin{bmatrix}1.0\\ 0.8\end{bmatrix}, C=\begin{bmatrix}-0.2\\ 0\end{bmatrix}^{\top}.$$

The Laplacian matrix is selected as follows:

$$L=\begin{bmatrix}-1 & 1 & 0 & 0 & 0 & 0\\ 1 & -4 & 1 & 0 & 1 & 1\\ 0 & 1 & -2 & 0 & 0 & 1\\ 0 & 0 & 0 & -1 & 1 & 0\\ 0 & 1 & 0 & 1 & -3 & 1\\ 0 & 1 & 1 & 0 & 1 & -3\end{bmatrix}.$$

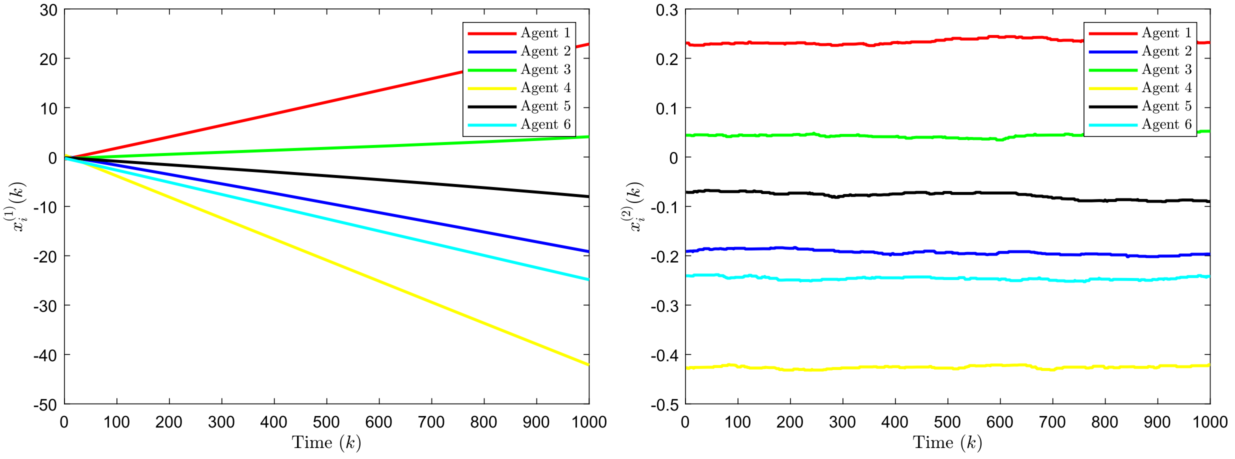
Under the MRRP, the system matrices in (23) switch periodically with $r(k)$. The number of neighboring nodes selected to obtain communication permissions with agent i is denoted as S_i, and $S_1=1, S_2=2, S_3=2, S_4=1, S_5=2, S_6=2$. With the help of formula (4) and the definition of T, it is not difficult to derive the minimal period of the periodic controller is $T=6$.

Fig. 4 and Fig. 5 plot the operating state of the system under the open loop condition and closed loop condition, respectively. Obviously, under open loop situation, the DMASs cannot reach the expected consensus control scheme. To illustrate the cyber attacks on the system performance and the verify the effectiveness of the designed controller, next, simulation results will be provided with and without cyber attacks.

Case 1: When the MASs are affected by hybrid cyber attacks, let $\tilde{\epsilon}=\sqrt{1.16}$, $\chi_0^2=2$, $\bar{\lambda}_i=0.1$ and $\bar{\theta}_i=0.1$ $(i=1,2,\cdots,6)$. By applying MATLAB software, we get a series of feasible solutions by Theorem 2:

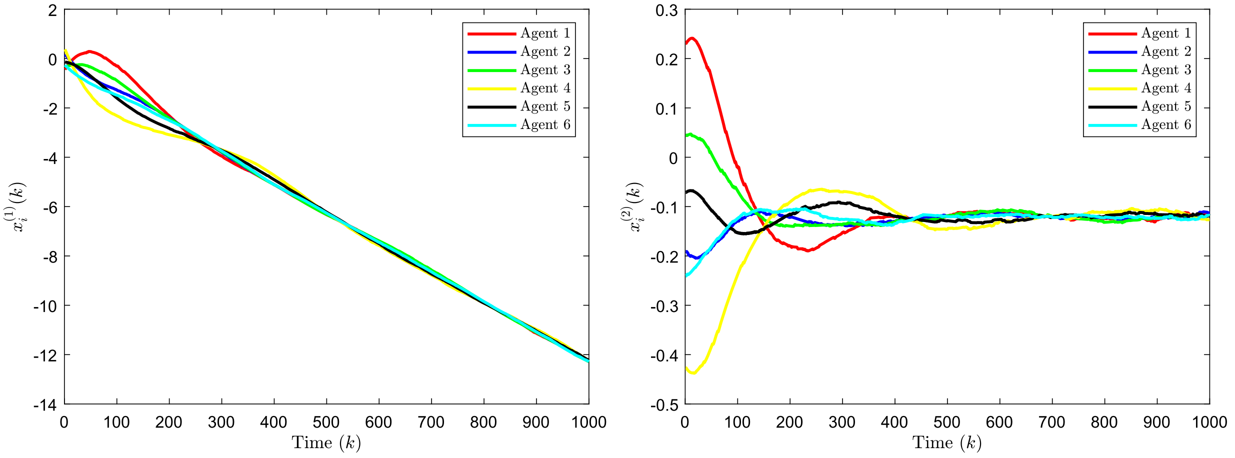
$$\hat{A}_1=\begin{bmatrix}-0.0180 & -0.0016\\ 0.0329 & -0.1799\end{bmatrix}, \hat{A}_2=\begin{bmatrix}-0.0193 & -0.0017\\ 0.0331 & -0.1799\end{bmatrix}, \hat{A}_3=\begin{bmatrix}-0.0173 & -0.0016\\ 0.0328 & -0.1799\end{bmatrix},$$
$$\hat{A}_4=\begin{bmatrix}-0.0183 & -0.0016\\ 0.0330 & -0.1799\end{bmatrix}, \hat{A}_5=\begin{bmatrix}-0.0183 & -0.0016\\ 0.0329 & -0.1799\end{bmatrix}, \hat{A}_6=\begin{bmatrix}-0.0180 & -0.0016\\ 0.0329 & -0.1799\end{bmatrix},$$
$$\hat{L}_1=\begin{bmatrix}0.2612 & -0.0682\end{bmatrix}^{\top}, \hat{L}_2=\begin{bmatrix}0.2804 & -0.0730\end{bmatrix}^{\top}, \hat{L}_3=\begin{bmatrix}0.2514 & -0.0657\end{bmatrix}^{\top},$$
$$\hat{L}_4=\begin{bmatrix}0.2664 & -0.0695\end{bmatrix}^{\top}, \hat{L}_5=\begin{bmatrix}0.2664 & -0.0695\end{bmatrix}^{\top}, \hat{L}_6=\begin{bmatrix}0.2612 & -0.0682\end{bmatrix}^{\top},$$
$$\hat{K}_1=\begin{bmatrix}-0.3570 & -0.0588\end{bmatrix}, \hat{K}_2=\begin{bmatrix}-0.3556 & -0.0588\end{bmatrix}, \hat{K}_3=\begin{bmatrix}-0.3576 & -0.0588\end{bmatrix},$$
$$\hat{K}_4=\begin{bmatrix}-0.3567 & -0.0588\end{bmatrix}, \hat{K}_5=\begin{bmatrix}-0.3566 & -0.0588\end{bmatrix}, \hat{K}_6=\begin{bmatrix}-0.3570 & -0.0588\end{bmatrix}.$$

During the simulation process, all elements of $x_i(0)$ $(i=1,2,\cdots,6)$ are randomly selected obeying uniform distribution $\mathcal{U}[-0.5,0.5]$ with $\chi_0^2=2$. Deception and injection attack information is expressed by $0.1sin(\alpha_i(k))$ and $0.01sin(\beta_i(k))$, where $\alpha_i(k)$ and $\beta_i(k)$ obey the Gaussian distribution $\mathcal{N}(2,4)$ and normal distribution $\mathcal{N}(0,1)$, respectively. Under the designed control method, the state deviation of each agent from the average state is shown in Fig. 6. Fig. 7 plots the moments at which y_i and u_i suffer cyber attacks. It can be observed that the controlled closed loop MASs could reach the desired consensus state when the MASs suffer hybrid attacks.



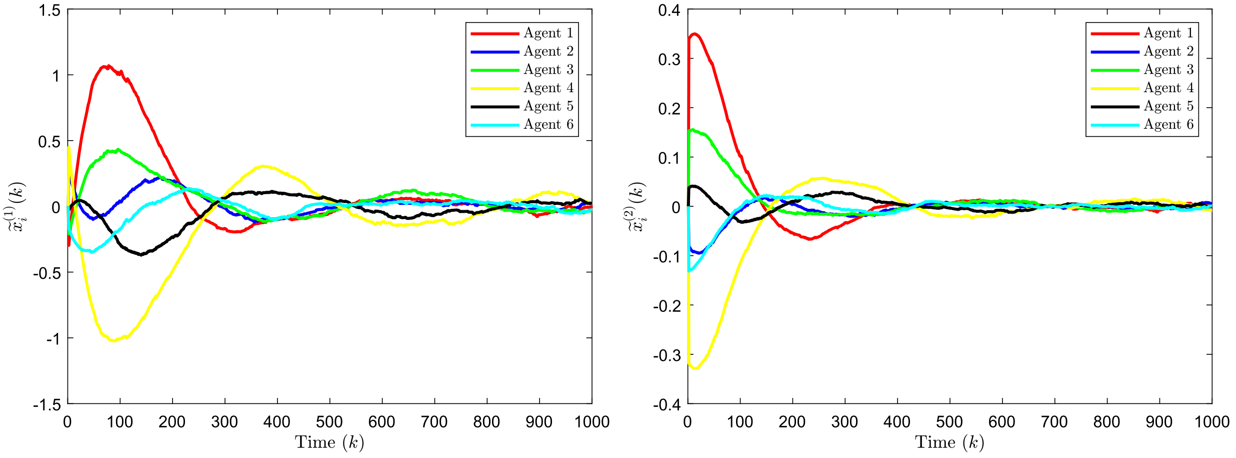
(a) (b)

Fig. 4. The state trajectories of the DMASs without control strategy.



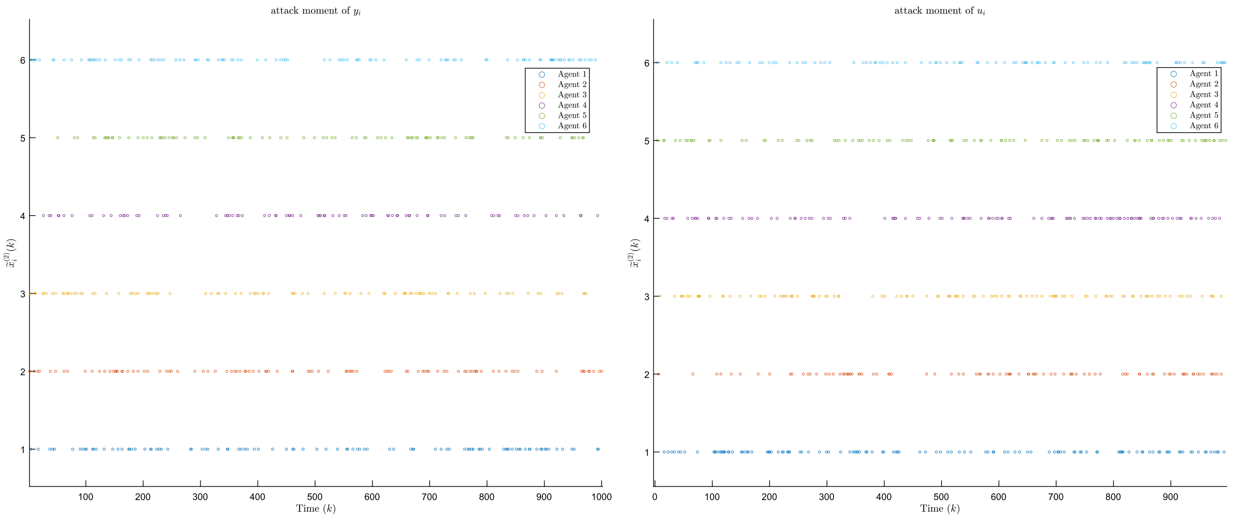
(a) (b)

Fig. 5. The state trajectories of the DMASs with control strategy.



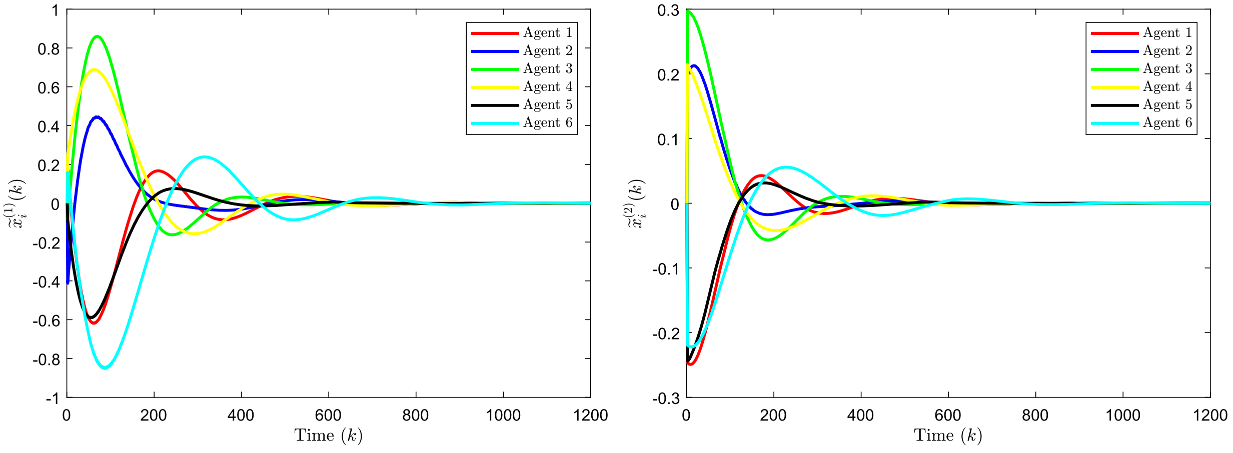
(a) (b)

Fig. 6. Consensus error under MRRP with cyber attacks.



(a) (b)

Fig. 7. The attack moment of y_i and u_i.



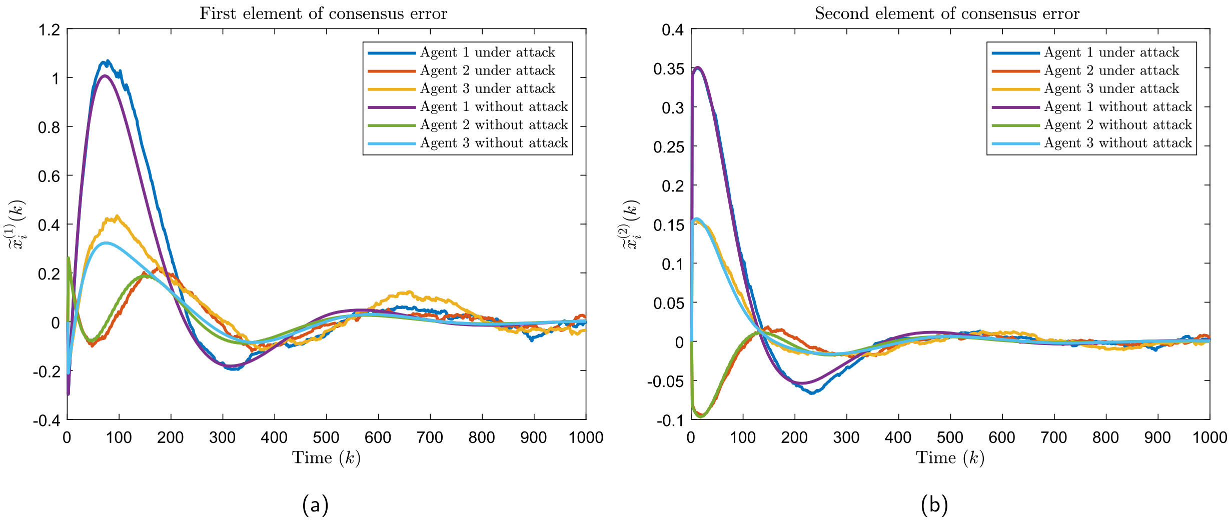
(a) (b)

Fig. 8. Consensus error under MRRP without cyber attacks.

Case 2: When the MASs are without hybrid cyber attacks, the values of $\widetilde{\epsilon}$, χ_0^2, $\overline{\lambda}_i$ and $\overline{\theta}_i$ $(i = 1, 2, \cdots, 6)$ are chosen the same as in Case 1, the observer and controller gains can be solved similarly as follows

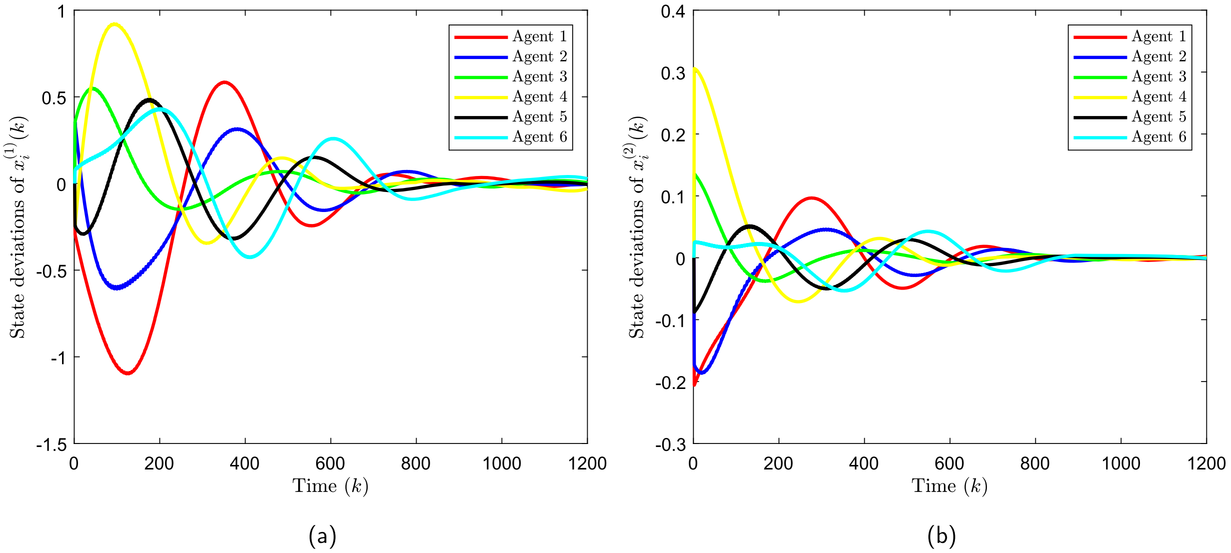
$$\hat{A}_1 = \begin{bmatrix} -0.0221 & -0.0017 \\ 0.0333 & -0.1799 \end{bmatrix}, \hat{A}_2 = \begin{bmatrix} -0.0226 & -0.0018 \\ 0.0334 & -0.1799 \end{bmatrix}, \hat{A}_3 = \begin{bmatrix} -0.0215 & -0.0017 \\ 0.0332 & -0.1799 \end{bmatrix},$$
$$\hat{A}_4 = \begin{bmatrix} -0.0223 & -0.0017 \\ 0.0334 & -0.1799 \end{bmatrix}, \hat{A}_5 = \begin{bmatrix} -0.0228 & -0.0018 \\ 0.0334 & -0.1799 \end{bmatrix}, \hat{A}_6 = \begin{bmatrix} -0.0212 & -0.0017 \\ 0.0332 & -0.1799 \end{bmatrix},$$
$$\hat{L}_1 = \begin{bmatrix} 0.2895 & -0.0741 \end{bmatrix}^\top, \hat{L}_2 = \begin{bmatrix} 0.2965 & -0.0758 \end{bmatrix}^\top, \hat{L}_3 = \begin{bmatrix} 0.2818 & -0.0722 \end{bmatrix}^\top,$$
$$\hat{L}_4 = \begin{bmatrix} 0.2914 & -0.0746 \end{bmatrix}^\top, \hat{L}_5 = \begin{bmatrix} 0.2986 & -0.0763 \end{bmatrix}^\top, \hat{L}_6 = \begin{bmatrix} 0.2781 & -0.0713 \end{bmatrix}^\top,$$
$$\hat{K}_1 = \begin{bmatrix} -0.3525 & -0.0588 \end{bmatrix}, \hat{K}_2 = \begin{bmatrix} -0.3519 & -0.0588 \end{bmatrix}, \hat{K}_3 = \begin{bmatrix} -0.3530 & -0.0588 \end{bmatrix},$$
$$\hat{K}_4 = \begin{bmatrix} -0.3523 & -0.0588 \end{bmatrix}, \hat{K}_5 = \begin{bmatrix} -0.3517 & -0.0588 \end{bmatrix}, \hat{K}_6 = \begin{bmatrix} -0.3533 & -0.0588 \end{bmatrix}.$$

Choose the same initial condition as in Case 1, the consensus error trajectory graph for the DMASs under MRRP in the absence of cyber attacks is shown in Fig. 8, which shows the effectiveness of the proposed method. To show the effects of the cyber attacks on the system performance, the consensus error of Agent 1, 2 and 3 in the presence and absence of attacks is plotted in Fig. 9, the consensus error of Agent 4, 5 and 6 can be drawn similarly, which is omitted here. The comparisons of the MRRP and RRP on the



(a) (b)

Fig. 9. Consensus error under MRRP with and without cyber attacks.



(a) (b)

Fig. 10. Consensus error under RRP without cyber attacks.

system performance are illustrated in Fig. 8 and Fig. 10, from the two figures, we can see that the agents can achieve consensus more quickly under MRRP than under RRP.

The above simulation results conform that MRRP fully leverages the available communication channels, enabling a faster convergence speed and thereby facilitating a more rapid achievement of consensus. The proposed control strategy is effective, and has a certain resistance to the cyber attacks, thus proving that the system has a good robustness and can finally achieve consensus.

5. Conclusion

This paper has discussed the consensus control for DMASs subject to MRRP under complex hybrid attacks, where MRRP has been firstly implemented to achieve reasonable allocation of the network resources during information transmission among agents. The influences of the cyber attacks on the transmitted sensor and actuator input are both considered in constructing the closed-loop system. The sufficient condition ensuring the desired consensus performance of the MASs has been derived and the design method of the distributed observer and controller are presented. Finally, simulation results have been applied to confirm the effectiveness of the presented approach. In the future, the anti-disturbance bipartite consensus control for MASs will be explored considering the proposed MRRP in this paper.

CRediT authorship contribution statement

Jinliang Liu: Writing – review & editing, Supervision, Funding acquisition. **Hao Zheng:** Writing – original draft, Software. **Lijuan Zha:** Writing – review & editing, Funding acquisition. **Engang Tian:** Writing – review & editing, Formal analysis. **Chen Peng:** Writing – review & editing, Investigation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgement

This work was supported in part by the National Natural Science Foundation of China under Grants 62273174 and 62373252, in part by the Natural Science Foundation of Jiangsu Province of China under Grants BK20230063.

References

[1] Angelo Coppola, Dario Giuseppe Lui, Alberto Petrillo, Stefania Santini, Cooperative driving of heterogeneous uncertain nonlinear connected and autonomous vehicles via distributed switching robust pid-like control, Inf. Sci. 625 (2023) 277–298.

[2] Ji Chol, Cha Ryong Gun, Multi-agent based scheduling method for tandem automated guided vehicle systems, Eng. Appl. Artif. Intell. 123 (2023) 106229.

[3] Wenbing Tang, Yuan Zhou, Yang Liu, Zuohua Ding, Jing Liu, Robust motion planning for multi-robot systems against position deception attacks, IEEE Trans. Inf. Forensics Secur. 19 (2024) 2157–2170.

[4] Guanglei Zhao, Hailong Cui, Changchun Hua, Hybrid event-triggered bipartite consensus control of multiagent systems and application to satellite formation, IEEE Trans. Autom. Sci. Eng. 20 (3) (2023) 1760–1771.

[5] Vincenzo Loia, Stefania Tomasiello, Alfredo Vaccaro, Using fuzzy transform in multi-agent based monitoring of smart grids, Inf. Sci. 388–389 (2017) 209–224.

[6] Zhenhua Deng, Jin Luo, Tao Chen, Distributed strategy for constrained resource allocation problems of autonomous second-order nonlinear agents and its application to smart grids, Inf. Sci. 652 (2024) 119754.

[7] Hossein Ehya, Tarjei N. Skreien, Arne Nysveen, Intelligent data-driven diagnosis of incipient interturn short circuit fault in field winding of salient pole synchronous generators, IEEE Trans. Ind. Inform. 18 (5) (2022) 3286–3294.

[8] Meina Zhai, Qiuye Sun, Bingyu Wang, Zhenwei Liu, Huaguang Zhang, Cooperative fault-estimation-based event-triggered fault-tolerant voltage restoration in islanded ac microgrids, IEEE Trans. Autom. Sci. Eng. 20 (3) (2023) 1829–1837.

[9] Yajian Zhang, Chen Peng, Chuanliang Cheng, Yu-Long Wang, Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks, IEEE Trans. Smart Grid 14 (2) (2023) 1223–1235.

[10] Li Zan, Yingnan Pan, Tianjiao An, Bo Dong, Xiaogang Dong, Global precise consensus tracking control for uncertain multiagent systems in cooperation-competition networks, Inf. Sci. 658 (2024) 120006.

[11] S. Zhu, J. Zhou, X. Yu, J.A. Lu, Bounded synchronization of heterogeneous complex dynamical networks: a unified approach, IEEE Trans. Autom. Control 66 (4) (2021) 1756–1762.

[12] Yan Zong, Xuewu Dai, Zhiwei Gao, Proportional–integral synchronization for nonidentical wireless packet-coupled oscillators with delays, IEEE Trans. Ind. Electron. 68 (11) (2021) 11598–11608.

[13] Wei Chen, Derui Ding, Hongli Dong, Guoliang Wei, Xiaohua Ge, Finite-horizon $\mathcal{H}_\infty$ bipartite consensus control of cooperation–competition multiagent systems with round-Robin protocols, IEEE Trans. Cybern. 51 (7) (2021) 3699–3709.

[14] Wei Zhang, Qian Huang, Adi Alhudhaif, Event-triggered fixed-time bipartite consensus for nonlinear disturbed multi-agent systems with leader-follower and leaderless controller, Inf. Sci. 662 (2024) 120243.

[15] Hong-Xiang Hu, Guanghui Wen, Guang Chen, Yun Chen, Xinghuo Yu, Output bipartite consensus for second-order heterogeneous uncertain agents with state-dependent cooperation-competition interactions, IEEE Trans. Control Netw. Syst. 10 (2) (2023) 912–925.

[16] Dipankar Maity, Panagiotis Tsiotras, Multiagent consensus subject to communication and privacy constraints, IEEE Trans. Control Netw. Syst. 9 (2) (2022) 943–955.

[17] Xiang-Gui Guo, Dong-Yu Zhang, Jian-Liang Wang, Ju H. Park, Lei Guo, Observer-based event-triggered composite anti-disturbance control for multi-agent systems under multiple disturbances and stochastic fdias, IEEE Trans. Autom. Sci. Eng. 20 (1) (2023) 528–540.

[18] Ni Yang, Ruiyi Gao, Youzhi Feng, Huan Su, Event-triggered impulsive control for complex networks under stochastic deception attacks, IEEE Trans. Inf. Forensics Secur. 19 (2024) 1525–1534.

[19] Rui Gao, Jiangshuai Huang, Xiaojie Su, Ling Zhao, Adaptive control of strict-feedback nonlinear systems under denial-of-service: a synthetic analysis, IEEE Trans. Inf. Forensics Secur. 19 (2024) 2315–2327.

[20] Hao Shen, Yu-An Liu, Kaibo Shi, Ju H. Park, Jing Wang, Event-based distributed secondary control for ac islanded microgrid with semi-Markov switched topology under cyber-attacks, IEEE Syst. J. 17 (2) (2023) 2927–2938.

[21] Jian Liu, Jiachen Ke, Jinliang Liu, Xiangpeng Xie, Engang Tian, Outlier-resistant non-fragile control of nonlinear networked systems under dos attacks and multi-variable event-triggered sc protocol, IEEE Trans. Inf. Forensics Secur. 19 (2024) 2609–2622.

[22] Lijuan Zha, Rongfei Liao, Jinliang Liu, Xiangpeng Xie, Engang Tian, Jinde Cao, Dynamic event-triggered output feedback control for networked systems subject to multiple cyber attacks, IEEE Trans. Cybern. 52 (12) (2022) 13800–13808.

[23] Kaiyue Dong, Guang-Hong Yang, Huimin Wang, Estimator-based event-triggered output synchronization for heterogeneous multi-agent systems under denial-of-service attacks and actuator faults, Inf. Sci. 657 (2024) 119955.

[24] Weihai Zhang, Zunjie Yu, Xiushan Jiang, Event-triggered security consensus of continuous-time multi-agent systems against complex cooperative attacks, Inf. Sci. 662 (2024) 120260.

[25] Jinliang Liu, Nan Zhang, Lijuan Zha, Xiangpeng Xie, Engang Tian, Reinforcement learning based decentralized control for networked interconnected systems with communication and control constraints, IEEE Trans. Autom. Sci. Eng. (2023), https://doi.org/10.1109/TASE.2023.3300917.

[26] Hao Zhang, Yuan Fan, Jianbin Qiu, Consensus protocol for discrete-time linear multiagent systems with channel fadings: a dynamic event-based approach, IEEE Trans. Control Netw. Syst. 10 (1) (2023) 345–354.

[27] Yu-Ping Tian, Cheng-Lin Liu, Consensus of multi-agent systems with diverse input and communication delays, IEEE Trans. Autom. Control 53 (9) (2008) 2122–2128.

[28] Ya Zhang, Yu-Ping Tian, Consensus of data-sampled multi-agent systems with random communication delay and packet loss, IEEE Trans. Autom. Control 55 (4) (2010) 939–943.

[29] Amir Amini, Arash Mohammadi, Amir Asif, Ming Hou, Konstantinos N. Plataniotis, Fault-tolerant periodic event-triggered consensus under communication delay and multiple attacks, IEEE Syst. J. 16 (4) (2022) 6338–6349.

[30] Jierui Zhang, Hongwei Xia, Guangcheng Ma, Output-constrained fixed-time coordinated control for multi-agent systems with event-triggered and delayed communication, Inf. Sci. 659 (2024) 120086.

[31] Weihao Song, Zidong Wang, Jianan Wang, Jiayuan Shan, Particle filtering for a class of cyber-physical systems under round-Robin protocol subject to randomly occurring deception attacks, Inf. Sci. 544 (2021) 298–307.

[32] Cheng Gong, Guopu Zhu, Peng Shi, Secure and asynchronous filtering for piecewise homogeneous Markov jump systems with quantization and round-Robin communication, Inf. Sci. 640 (2023) 119032.

[33] Bin Wei, Engang Tian, Jinliang Liu, Xia Zhao, Probabilistic-constrained tracking control for stochastic time-varying systems under deception attacks: a round-Robin protocol, J. Franklin Inst. 358 (17) (November 2021) 9135–9157.

[34] Licheng Wang, Zidong Wang, Di Zhao, Yang Liu, Guoliang Wei, Recursive filtering for discrete-time stochastic complex networks under bit-rate constraints: a locally minimum variance approach, IEEE Trans. Autom. Control 69 (5) (2024) 3441–3448.

[35] Licheng Wang, Zidong Wang, Di Zhao, Guoliang Wei, Stabilization of linear discrete-time systems over resource-constrained networks under dynamical multiple description coding scheme, Automatica 156 (2023) 111160.

[36] Hongchenyu Yang, Chen Peng, Zhiru Cao, Attack-model-independent stabilization of networked control systems under a jump-like tod scheduling protocol, Automatica 152 (2023) 110982.

[37] Lei Zou, Zidong Wang, Huijun Gao, Fuad E. Alsaadi, Finite-horizon $\mathcal{H}_\infty$ consensus control of time-varying multiagent systems with stochastic communication protocol, IEEE Trans. Cybern. 47 (8) (2017) 1830–1840.

[38] Jinliang Liu, Enyu Gong, Lijuan Zha, Engang Tian, Xiangpeng Xie, Observer-based security fuzzy control for nonlinear networked systems under weighted try-once-discard protocol, IEEE Trans. Fuzzy Syst. 31 (11) (2023) 3853–3865.

[39] Yamei Ju, Guoliang Wei, Derui Ding, Shuai Liu, A novel fault detection method under weighted try-once-discard scheduling over sensor networks, IEEE Trans. Control Netw. Syst. 7 (3) (2020) 1489–1499.

[40] Jinliang Liu, Enyu Gong, Lijuan Zha, Engang Tian, Xiangpeng Xie, Interval type-2 fuzzy-model-based filtering for nonlinear systems with event-triggering weighted try-once-discard protocol and cyber-attacks, IEEE Trans. Fuzzy Syst. 32 (3) (2024) 721–732.

[41] Yuxuan Shen, Zidong Wang, Bo Shen, Hongli Dong, Outlier-resistant recursive filtering for multisensor multirate networked systems under weighted try-once-discard protocol, IEEE Trans. Cybern. 51 (10) (2021) 4897–4908.

[42] Jinliang Liu, Enyu Gong, Lijuan Zha, Xiangpeng Xie, Engang Tian, Outlier-resistant recursive security filtering for multirate networked systems under fading measurements and round-Robin protocol, IEEE Trans. Control Netw. Syst. 10 (4) (2023) 1962–1974.

[43] Derui Ding, Zidong Wang, Daniel W.C. Ho, Guoliang Wei, Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks, IEEE Trans. Cybern. 47 (8) (2017) 1936–1947.

[44] Jiancun Wu, Chen Peng, Jin Zhang, Engang Tian, A sampled-data-based secure control approach for networked control systems under random dos attacks, IEEE Trans. Cybern. (2024) 1–11, https://doi.org/10.1109/TCYB.2024.3350331.